PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-333888

(43)Date of publication of application : 20.11.1992

---

(51)Int.Cl. G09C 1/00

G06F 12/14

H04L 9/00

H04L 9/10

H04L 9/12

---

(21)Application number : 03-104579 (71)Applicant : HITACHI LTD

(22)Date of filing : 10.05.1991 (72)Inventor : AISAKA KAZUO

HASHIZUME AKIHIDE

TAKASUGI KAZUO

FUNO TAKAKAZU

---

(54) INFORMATION PROTECTING METHOD AND CIPHERING DEVICE USING THE SAME

(57)Abstract:

PURPOSE: To realize the information protecting method and ciphering device which have high evidence ability by disabling both an information sender and a receiver to forge information.

CONSTITUTION: An electronic signature method which uses open key ciphers makes the ciphering key of signature information secret even to the sender. Consequently, the information sender ciphers the signature information 10 with the secret key by using a closed ciphering device 1 and sends the ciphered information to the receiver together with the original information. The receiver deciphers it by using the open key to confirm the information sender. Further, the

time when the ciphered signature is generated is included in the signature by a composing circuit 14 to prevent the sender from generating wrong information.

LEGAL STATUS [Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平4－333888

(43)公開日　平成４年(1992)11月20日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00		7922－5L		
Ｇ０６Ｆ　12/14	３２０　Ｂ	8841－5B		
Ｈ０４Ｌ　9/00				
9/10				
		7117－5K	Ｈ０４Ｌ　9／00	Ｚ

審査請求　未請求　請求項の数４(全　６　頁)　最終頁に続く

(21)出願番号　特願平3－104579

(22)出願日　平成３年(1991)５月10日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　相坂　一夫
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(72)発明者　橋詰　明英
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(72)発明者　高杉　和夫
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(74)代理人　弁理士　磯村　雅俊

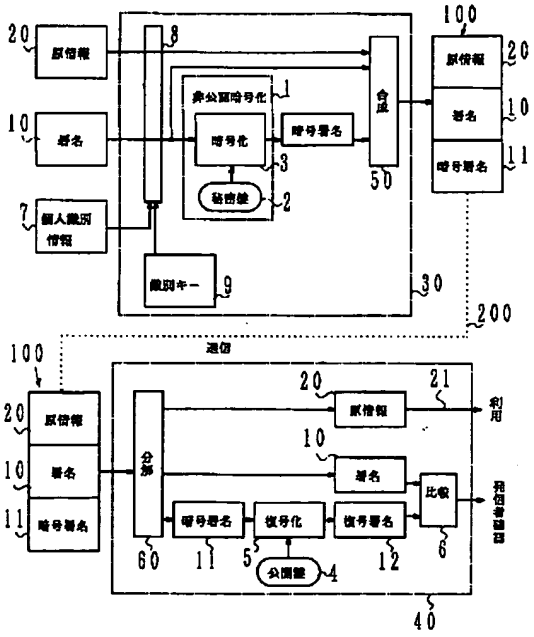
最終頁に続く

(54)【発明の名称】　情報保護方法およびそれを用いた暗号化装置

(57)【要約】

【目的】　情報の発信者および受信者の双方ともに、情報の偽造が不可能となり、証拠能力の高い情報保護方法および暗号化装置を実現できる。

【構成】　公開鍵暗号を用いる電子署名方法において、署名情報の暗号化鍵を発信者にも秘密にする。これにより、情報の発信者は、署名情報を非公開暗号化装置を用いて秘密鍵により暗号化を施し、原情報とともに受信者に送信する。受信者は公開鍵を用いて復号することにより情報の発信者を確認することができる。また、署名の中に暗号署名を作成した時刻を合成回路により含ませることにより、発信者が時刻を偽った情報を作成することを防止する。



1

【特許請求の範囲】

【請求項1】　電子情報の発信者を特定するための署名情報を暗号化し、暗号化された署名情報を原情報に添付して受信者に送信する情報保護方法において、署名情報を暗号化する処理を発信者に対して暗号化鍵を秘密にした状態で行い、暗号化された署名情報と入力されたままの署名情報とを原情報に添付して送信することを特徴とする情報保護方法。

【請求項2】　請求項1に記載の情報保護方法において、上記暗号化された署名情報には、該署名情報を暗号化した時刻を含ませることを特徴とする情報保護方法。

【請求項3】　署名情報を入力する入力手段と、該署名情報を暗号化した時刻を決定する計時手段と、該署名情報と該時刻とを合成する合成手段と、該合成手段で合成した情報を非公開暗号化方式を用いて暗号化する暗号化手段と、該暗号化手段に入力するための秘密鍵を記憶する手段と、該暗号化手段により暗号化された署名情報を出力する出力手段とを、筐体内に内蔵することを特徴とする暗号化装置。

【請求項4】　請求項3に記載の暗号化装置において、上記暗号化すべき署名情報を数値化した値Ｎで表すとき、次式で定められる変換により得られる数値Ｃを暗号として用いることを特徴とする暗号化装置。

Ｃ＝（Ｎ＊＊ｒ）ｍｏｄ　ｍ

なお、＊＊はべき乗、ｍｏｄは剰余、ｒは適当に定められた定数である。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、証拠能力が要求される情報を電子的に記録する装置において、記録の改ざんを防止することにより、情報を保護する方法、およびその方法を用いた暗号化装置に関する。

【０００２】

【従来の技術】証拠能力が要求される情報としては、例えば、医師により作成されたカルテ、納税者により作成された納税申告書、銀行により作成された借用明細書、発明者により作成された特許明細書および図面等がある。最近では、これらの書類をフレキシブルディスク、磁気テープ、固定ディスク等の電子媒体に記録する方法が用いられている。また、これらの書類は、電子的に記録された後、通信手段により遠隔地に通信されて、関係者に渡されたり、または会社や官庁に届けられることが多い。電子媒体を用いた情報の記憶、および通信に際しては、情報が作為的に改ざんされて悪用されるおそれがあるため、それを防ぐ方法が必要となる。従来の方法としては、例えば、嵩忠雄著『暗号アルゴリズムと計算量の理論』、情報処理、第２５巻６号、pp.547～553(1984年6月発行)に記載されている方法が用いられている。これによれば、従来の情報保護方法は、次のようなものであった。

2

（イ）第１の方法は、情報発信者を特定する何等かの符号を暗号化したものを、その情報に付加して送信（または記憶）する方法である。情報の受信者（すなわち、再生者）は、暗号化された符号を解読することにより、受信した情報が正当な発信者から送られたものであることを検証することができる。従って、第１の方法は、情報の信憑性を確認するために有効である。しかしながら、この方法は、発信者と受信者との間に信頼関係がある場合にのみ有効な方法である。何故ならば、受信者等が発信者を装って、情報を改ざんし、符号を暗号化することが可能であるからである。すなわち、通常の暗号化方法では、暗号の解読方法から暗号化方法を推定することができるので、受信者が発信者を装って情報を作成することが可能となり、第三者が情報の発信者を特定することは不可能となる。

（ロ）第２の方法は、第１の方法の欠点を除くために考えられたものであって、電子署名方法という名称で知られている方法である。これは、近年開発された一方通行型の暗号化方法を応用したものである。一方通行型の暗号化方法とは、暗号の解読方法を知り得ても、そこから暗号化方法を推定することが不可能な方法であって、例えばＲＳＡ暗号方式（後述の方式）がある。この一方通行型の暗号化方法を用いることにより、受信者による情報の偽造を防止することが可能である。

【０００３】

【発明が解決しようとする課題】このように、従来から用いられてきた情報の改ざん防止方法では、情報を受信者や第三者により偽造されることを防止することはできるが、情報が発信者自らの手で変造されることを防止することはできない。例えば、カルテを担当の医師が改ざんしたり、銀行により借用内容が改ざんされたり、発明者により明細書が改ざんされると、本人または関係者、さらには社会全体が大きな影響を受けることになり、このようなことは全体に防止しなければならない。このような電子情報が裁判等の証拠として利用される場合に、この電子情報が発信者の手で変造された物である可能性は否定できず、その結果、証拠能力に疑問が生じる。本発明の目的は、このような従来の課題を解決し、発信者にとっても電子情報を変造できないようにして、電子情報を安全に保護することができる情報保護方法およびそれを用いた暗号化装置を提供することにある。

【０００４】

【課題を解決するための手段】上記目的を達成するため、本発明の情報保護方法は、（イ）署名情報を暗号化する処理を発信者に対して暗号化鍵を秘密にした状態で行い、暗号化された署名情報と入力されたままの署名情報とを原情報に添付して送信することに特徴がある。また、（ロ）暗号化された署名情報には、署名情報を暗号化した時刻を含ませることにも特徴がある。また、その情報保護方法を用いた暗号化装置は、（ハ）署名情報を

3

入力する入力手段と、署名情報を暗号化した時刻を決定する計時手段と、署名情報と時刻とを合成する合成手段と、合成手段で合成した情報を非公開暗号化方式を用いて暗号化する暗号化手段と、暗号化手段に入力するための秘密鍵を記憶する手段と、暗号化手段により暗号化された署名情報を出力する出力手段とを、筐体内に内蔵することに特徴がある。また、（二）暗号化すべき署名情報を数値化した値Nで表すとき、次式で定められる変換により得られる数値Cを暗号として用いることにも特徴がある。

C＝（N＊＊r）mod　m

なお、＊＊はべき乗、modは剰余、rは適当に定められた定数である。

【0005】

【作用】本発明においては、暗号化方法を発信者および受信者のいずれでもない第三者である管理者が管理することにより、暗号化方法を情報の発信者からも隠蔽することができる。管理者は、発信者に暗号化装置を提供するが、暗号化の方法は開示しないようにする。また、管理者は情報の受信者に対して暗号の解読装置を提供するが、その解読装置から暗号化の方法が推定できないように、暗号化の方法として一方通行型の暗号化方法を用いる。これにより、情報の発信者、受信者の双方が暗号化方法を知ることができない。その結果、発信者が一度発信した情報は、発信者本人といえども改ざんが不可能となるため、情報の証拠能力は向上する。

【0006】

【実施例】以下、本発明の実施例を図面により詳細に説明する。図1は、本発明の第1の実施例を示す暗号化による情報保護システムのブロック図である。図1において、30は送信側装置であって、1は非公開暗号化装置、2は秘密鍵、3は暗号化計算回路、8はインヒビット回路、9は識別キー、11は暗号署名情報、50は合成回路である。この送信側装置30の入出力側における10は署名情報、7は個人識別情報、100は送信内容、20は原情報、10は署名情報、11は暗号署名情報である。また、40は受信側装置であって、60は情報分解回路、11は暗号署名情報、5は復号化回路、4は公開鍵、20は原情報、10は署名情報、12は復号署名情報、7は個人識別情報、6は比較回路である。また、200は送信側装置30と受信側装置40とを結ぶ通信路である。本実施例においては、原情報20に加えて署名情報10と個人識別情報7とを送信側装置30に入力することにより、情報の発信者を特定する。すなわち、個人識別情報7が入力されると、装置30内の識別キー9の内容も入力されることにより、両者が不一致のときにはインヒビットされ、原情報20と署名情報10の入力ができなくなる。そして、非公開暗号化装置1の内容は発信者であっても見ることができないため、一旦作成し送信した情報は、発信者といえども改ざんすることは不可能である。個人識別情報7と識別キー9が一致すると、原情報20はそのまま合成回路50に送られるとともに、署名情報10はそのままの形式と、暗号化計算装置3で秘密鍵2により暗号化された後、暗号署名情報11の形式となって、いずれも合成回路50に送られる。3種類の原情報20、署名情報10、および暗号署名情報11は、合成回路50により1つの情報にまとめられて、複合情報100として通信路200を介して受信側装置40に送信される。

4

【0007】複合情報100が受信側装置40に受信されると、先ず分解回路60で複合情報100を原情報20、署名情報10、および暗号署名情報11の3種類に分解する。これらのうち、原情報20はそのまま出力回路21により出力されて、受信者により利用される。また、署名情報10は、情報発信者を確認するために、次のように利用される。すなわち、先ず暗号署名情報11は、復号化のための計算回路5により復号署名情報12に復号される。計算には、公開されている復号化鍵4が用いられる。復号署名情報12と暗号化されていない署名情報10とは、比較回路6で比較され、両者が一致すれば情報が正当な発信者からのものであることが確認できる。このように、比較の結果は、発信者の確認情報として出力される。

【0008】図2は、本発明の第2の実施例を示す情報保護システムのブロック図である。本実施例では、暗号化の時刻を署名情報に合成して送信することにより、その時刻を不変にして、情報の改ざんを防止できるようにする。図2において、図1の他に新たに付加された機能は、非公開暗号化装置1内の計時回路である上昇カウンタ13と合成回路14であり、また受信側装置40内の復号化回路5により復号署名情報12と計時情報13に復号化されることである。図2では、原情報20と署名情報10のみを送信側装置30に入力することにより、原情報20はそのまま合成回路50に送られる。一方、署名情報10は、非公開暗号化装置1で暗号署名情報11に暗号化される際に、暗号化の計時情報13も合成される。すなわち、非公開暗号化装置1は、入力された署名情報10と計時カウンタ13の計時情報を合成回路14で合成されたものに対して、暗号化回路3で秘密鍵2により暗号化する。暗号化された暗号署名情報11と暗号化されないままの署名情報10と原情報20とは、合成回路50で合成されて複合情報100となる。原情報20と署名情報10と暗号署名情報11からなる複合情報100は、通信路200を介して送信側装置30から受信側装置40に送信される。受信側装置40では、復号化のための計算回路5において、復号署名情報12とともに暗号化の時刻13を得ることが可能となる。すなわち、複合情報100は、分解回路60で原情報20と署名情報10と暗号署名情報11とに分解された後、原情報20はそのまま出力されて受信者に利用される。ま

5

た、暗号署名情報１１は、復号化回路５で公開鍵４により復号化され、復号署名情報１２と計時情報１３とに復号される。そして、計時情報１３は発信時刻の確認のために出力され、復号署名情報１２は署名情報１０とともに比較回路６に入力されて、一致すれば情報が正当な発信者からのものであることが確認される。この結果、一度発信した情報を過去に遡って訂正することが不可能となり、より証拠性の高い情報が得られることになる。

【０００９】図３は、図２における非公開暗号化装置の詳細ブロック図である。非公開暗号化装置１は、合成回路１４、上昇カウンタ（計時）１３１、演算ユニット３、および秘密鍵記憶回路２を備えている。上昇カウンタ１３１は、外部からのクロック入力１３０により計時回路として動作する。上昇カウンタ１３１を上昇専用とすることにより過去の時刻を装って情報の偽造を防止することができる。合成回路１４は、外部からの署名入力１４０および上昇カウンタ１３１の両者の出力を１つに合成して演算ユニット３に出力する。この合成により、署名情報を暗号化する時刻が署名情報と一体化されて演算ユニット３に送られるので、暗号化の結果得られる暗号署名において、時刻の情報のみを改ざんして情報の発信時刻を偽ることは不可能となる。なお、演算ユニット３は、乗算、剰余の算出、計算途中結果の記憶等の記能を有している。

【００１０】演算ユニット３は、合成回路１４で合成された結果の出力を受け取ると、秘密鍵記憶回路２に記憶されている暗号化のための秘密鍵を用いて合成回路１４からの出力を暗号署名に変換し、暗号署名出力３０を取り出す。これらの各回路は、物理的に開封が困難な筐体にまとめられて格納されるので、情報の発信者にもそれらの内容を知られることがない。また、秘密鍵記憶回路２に記憶される内容は、筐体１を密封する前に予め書き込んでおく。この内容は、受信側で用いる公開鍵４により復号が行えるように決定される。

【００１１】次に、本発明で用いられる公開鍵暗号法の一種であるＲＳＡ暗号方式について述べる。ＲＳＡ暗号とは、１９７８年に米国のリベスト（Rivest)等により提案された暗号方式であって、暗号の解読(複合化)方法が判っていても、そこから暗号化方法を推定することが事実上不可能であるという性質を有している。一般に暗号化方式とは、通常の言語で書かれた文章(平文)を暗号文に変換する規則のことである。ＲＳＡ暗号化方式は、この変換規則として数学の一分野である整数論の手法を応用した暗号方式であって、次のような変換規則を用いる。先ず、平文を適当な規則により数値Ｎに変換する。通常は、平文の計算機内部での表現（ビットパターン）を２進数値として解釈したものをＮとする。次に、得られた数値Ｎを以下の数式により数値Ｃに変換して、得られた数値Ｃを暗号文とする。

【数１】　Ｃ＝（Ｎ＊＊ｒ）ｍｏｄ　ｍ

6

ここで＊＊はべき乗を、ｍｏｄは剰余をとる演算を表わすものとする。また、ｒおよびｍは適当なパラメータであって、その決定方法は後述する。逆に、上記で得られた暗号文Ｃを平文Ｎに復号化する（解読する）ためには、以下の数式を用いて変換すればよい。

【数２】　Ｎ＝（Ｃ＊＊ｓ）ｍｏｄ　ｍ

ここで、ｒ、ｓはそれぞれ以下の数式を満足するように選択される。

【数３】　（ｒ×ｓ）ｍｏｄ　φ（ｍ）＝１

ただし、φはオイラーの関数である。

【００１２】このＲＳＡ暗号化方式においては、２つの整数ｍおよびｒが暗号化のパラメータであり、またｍおよびｓが復号化のパラメータである。この方式の特質は、ｎを適切に選択すると、復号化のパラメータｍおよびｓが知られても、それらから暗号化パラメータｒを求めることが事実上不可能となる点である。このためには、ｍを２つの十分に大きな素数ｐ，ｑの積とする。ｓからｒを求めるためには、上記（数３）が示すようにオイラーの関数φ（ｍ）の値を計算する必要があるが、ｍ＝ｐ×ｑの場合には、次の数式が成立する。

【数４】　φ（ｍ）＝（ｐ－１）×（ｑ－１）

従って、φ（ｍ）の値を計算するには、ｍを素因数分解してｐ，ｑを求める必要がある。一方、素因数分解を十分高速に行う方法は存在しないことが経験的に知られている。その結果、ｐ，ｑを十分に大きく選択すれば、ｓからｒを求める計算は実用的な時間内には終了しないことになる。

【００１３】

【発明の効果】以上説明したように、本発明によれば、情報の発信者、受信者が双方とも情報を遡って偽造することが不可能であり、証拠能力の高い情報保護が可能となる。

【００１４】

【図面の簡単な説明】

【図１】本発明の第１の実施例を示す情報保護システムのブロック図である。

【図２】本発明の第２の実施例を示す情報保護システムのブロック図である。

【図３】図２で用いられる非公開暗号化装置の詳細ブロック図である。

【符号の説明】

１　非公開暗号化装置
２　秘密鍵記憶回路
３　暗号化計算回路
４　公開鍵記憶回路
５　復号化計算回路
６　比較回路
７　個人識別情報
８　インヒビット回路
９　識別キー

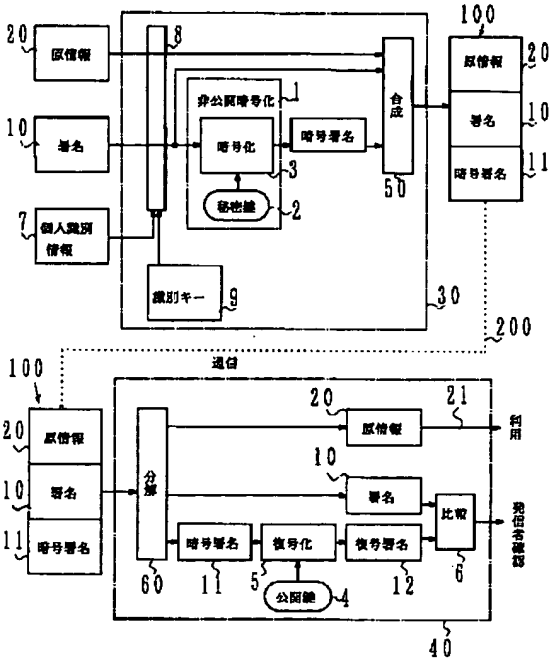
7

10　署名情報
11　暗号署名情報
12　復号署名情報
13　時計情報
14　合成回路
20　原情報
21　原情報の出力
30　暗号署名出力

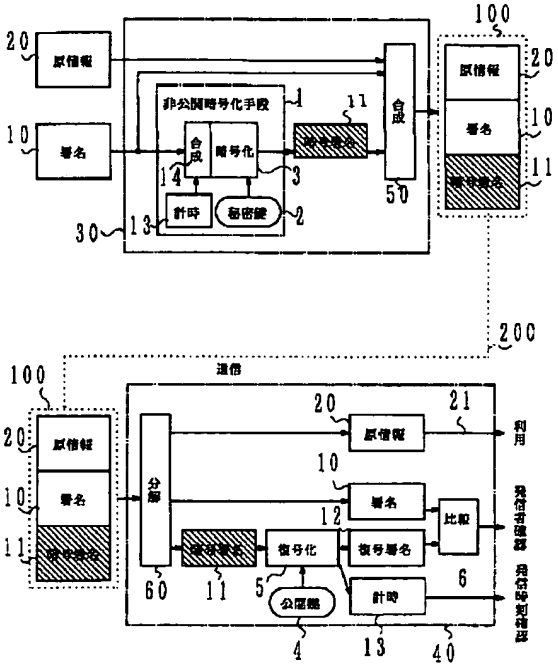
8

50　送信情報を合成する回路
60　受信情報を分解する回路
100　送信内容
130　クロック入力
131　上昇カウンタ
140　署名入力
200　通信路

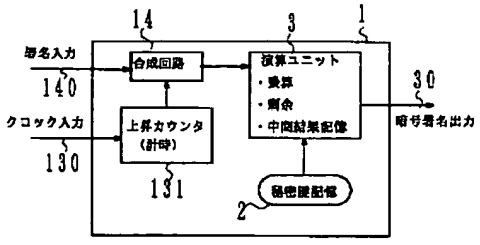
【図1】



【図2】



【図3】



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/12				

(72)発明者　布野　孝和
東京都国分寺市東恋ケ窪1丁目280番地
株式会社日立製作所中央研究所内